Innehåll

Grundläggande frågor vid personuppgiftsbehandling

Vad är en personuppgift?

Varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person. Exempel på personuppgifter är namn, adress, personnummer och samordningsnummer, telefonnummer, men även

annan information som kan kopplas till en viss person är personuppgifter som exempelvis e-postadress, bilder, ljudupptagning, patient-id, betalningsuppgifter som konto- eller betalkortsnummer samt uppgifter om en fysisk persons hälsa.

Vad är en känslig personuppgift?

En känslig personuppgift är en personuppgift som bedöms vara mer integritetskänslig än vanliga personuppgifter. GDPR anger att följande är känsliga personuppgifter:

- Etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
  - Även uppgift om att inte tro på något är en känslig personuppgift
- Medlemskap i fackförening
  - Även uppgift om att inte vara med i en fackförening är en känslig personuppgift
- Hälsa
- Sexualliv eller sexuell läggning
- Biometriska uppgifter
- Genetiska uppgifter

Varför säger man att vissa uppgifter är känsliga?

Varför anses vissa uppgifter vara känsliga? Det beror på att de har nära koppling till viktiga grundläggande och grundlagsskyddade fri- och rättigheter nämligen yttrandefrihet, informationsfrihet, mötesfrihet, föreningsfrihet, religionsfrihet, rätt till kroppslig integritet och rätt till privat- och familjeliv.

Begreppen i listan över känsliga personuppgifter kan tolkas brett och kan fånga upp information som kanske inte ses som särskilt känslig. Exempelvis är det sannolikt att uppgifter om en persons mentala hälsa är känsligare än uppgifter om att en person brutit benet men båda uppgifterna berör hälsa. Oavsett om du tycker att uppgiften är känslig så ska dessa uppgifter hanteras varsamt.

Vad är uppgifter om hälsa?

Uppgifter om hälsa ska tolkas brett. Det är uppgifter om en persons fysiska eller psykiska hälsa och tillhandahållande av hälso- och sjukvårdstjänster som ger information om personens hälsostatus.

Det kan vara personens tidigare, nuvarande eller framtida hälsotillstånd. Uppgifter om skada, sjukdom, funktionsvariation, diagnoser eller medicinsk historia. Provresultat, data från medicinska apparater såsom EKG eller data från fitness trackers är andra exempel. Även besöksdetaljer till en vårdinrättning är känsliga personuppgifter.

Vad är biometriska och genetiska uppgifter?

Biometriska uppgifter är uppgifter som erhållits genom särskild teknisk bearbetning som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifiering av personen. Exempelvis ansiktsigenkänning, fingeravtrycksuppgifter, röstigenkänning, hornhinneanalys, "keystroke analysis" (alltså att man analyserar hur någon skriver på ett tangentbord), handstilsanalys eller gånganalys.

Genetiska uppgifter är uppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken som ger information om hens fysiologi. Exempelvis analys av personens DNA, RNA eller annan form av analys som gör det möjligt att inhämta motsvarande information. Det är alltså resultatet av exempelvis ett blodprov som kan vara en känslig personuppgift och inte själva blodprovet.

Vad är behandling av personuppgifter?

En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter oberoende om det utförs automatiserat eller inte. Exempel på behandlingar är samla in, registrera, läsa, arkivera (spara i myndighetens arkiv) och lämna ut sådana uppgifter.

När får man behandla känsliga personuppgifter?

Som huvudregel får man enligt GDPR inte behandla känsliga personuppgifter. Dock finns många undantag som säger att man trots allt får behandla sådana personuppgifter.

VGR har i många verksamheter rätt att behandla känsliga personuppgifter eftersom det finns särskilt lagstöd för det. Känsliga personuppgifter ska dock alltid ges ett särskilt högt skydd mot obehörig åtkomst.

Ett exempel på då VGR har stöd i lag att behandla känsliga personuppgifter om hälsa är inom hälso- och sjukvården, där vi behöver behandla uppgifter om hälsa för att kunna erbjuda en god och patientsäker vård.

Särskilt skyddsvärda personuppgifter - Personnummer och samordningsnummer

Personnummer och samordningsnummer räknas till kategorin "särskilt skyddsvärda personuppgifter". Dessa uppgifter anses extra skyddsvärda och ska exponeras så lite som möjligt.

Personnummer och samordningsnummer får endast behandlas om:

1. det finns samtycke
2. det är motiverat med hänsyn till ändamålet med behandlingen
3. det är viktigt för en säker identifiering
4. något annat beaktansvärt skäl föreligger eller
5. det framgår av lag eller föreskrift

I Sverige använder vi ofta personnummer eller samordningsnummer för att säkerställa identifieringen av en person, alltså punkten 3 ovan. Men man bör vara restriktiv med behandlingen av personnummer och samordningsnummer och den personuppgiftsansvarige måste alltså göra en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som det kan innebära.

Personnummer och samordningsnummet får inte exponeras på internet. De får heller inte finnas på adressetiketter, i kuvertfönster eller i försändelser som sänds utan kuvert.

Fundera alltid en extra gång om du behöver behandla personnummer eller samordningsnummer, kanske räcker det med födelsenummer eller födelseår och initialer?

Observera att vi SKA behandla personnummer för våra patienter. Vi är skyldiga att säkerställa patientens identitet. Detta gäller även för patienter med skyddade personuppgifter.

Grundläggande principerna – Kärnan i GDPR

De grundläggande principerna är kärnan i GDPR. Principerna gäller för all personuppgiftsbehandling och sätter de yttersta ramarna för vad som är en tillåten behandling. Det är därför viktigt att du förstår principerna och tillämpar dem i din verksamhet när du behandlar personuppgifter. Ha alltid principerna i bakhuvudet när du arbetar med personuppgiftsbehandling.

De grundläggande principerna är:

- Laglighet, korrekthet, öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet

Vad innebär ”laglighet, korrekthet och öppenhet”?

All personuppgiftsbehandling måste vara laglig, korrekt och präglas av öppenhet. Att personuppgiftsbehandlingen ska vara laglig innebär att vi måste ha en *rättslig grund* för personuppgiftsbehandling (du kan läsa mer under rubriken ”rättslig grund”).

Personuppgiftsbehandlingen ska stå i rimlig proportion till den nytta som den innebär. Det ska vara klart och tydligt för de registrerade hur vi behandlar deras personuppgifter.

Vad innebär ”ändamålsbegränsning”?

Vi får bara samla in personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål (syftet med personuppgiftsbehandlingen).

Vad innebär ”uppgiftsminimering”?

Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet.

Vad innebär ”riktighet”?

Personuppgifter som behandlas ska vara riktiga och, om nödvändigt, uppdaterade. Om personuppgifterna inte stämmer ska vi rätta eller radera dem.

Vad innebär ”lagringsminimering”?

Vi får spara personuppgifter så länge som de behövs för ändamålet med personuppgiftsbehandlingen. När personuppgifterna inte längre behövs för ändamålet ska vi radera eller avidentifiera dem. I vissa fall måste vi spara handlingar som innehåller personuppgifter även efter det att vi slutat använda

dem. Det gäller till exempel bokföring, arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål samt statistiska ändamål.

För att få veta hur länge vi ska spara uppgifter, kolla i din förvaltnings informationshanteringsplan (tidigare dokumenthanteringsplan).

Hur länge får man spara personuppgifter?

Personuppgifter får som utgångspunkt inte sparas längre än vad som behövs för ändamålet som det behandlas.

När det gäller uppgifter som finns i allmänna handlingar – vilket omfattar flertalet av de uppgifter som hantera inom offentlig sektor (t ex VGR) - har offentlighetsprincipen och arkivlagen företräde. Enligt arkivlagen ska uppgifterna bevaras. Inom offentlig sektor finns gallringsrutiner för hur länge uppgifter i allmänna handlingar ska sparas. Arkivnämnden har beslutat att handlingar som är av "tillfällig eller ringa betydelse" får slängas. Varje nämnd och styrelse inom VGR har en dokumenthanteringsplan som reglerar detta.

Det är viktigt att inte spara uppgifter längre än de behövs för ändamålet eller informationshanteringsplan/gallringsrutin. Att spara register med personuppgifter för att det ”kan vara bra att ha” är inte tillåtet.

Vad innebär ”integritet” och ”konfidentialitet”?

När vi behandlar personuppgifter måste vi se till att uppgifterna skyddas på ett bra sätt genom att vidta lämpliga säkerhetsåtgärder. Alla personuppgifter som vi behandlar måste skyddas, så att ingen obehörig kommer åt dem och så att de inte används på ett otillåtet sätt. Vi ska också se till så att personuppgifter inte förloras eller blir förstörda, till exempel genom olyckshändelser. Vi måste därför införa lämpliga tekniska och organisatoriska säkerhetsåtgärder.

Rättsliga grunder

All behandling av personuppgifter som vi inom VGR utför måste vila på minst en av de rättsliga grunderna. Annars är behandlingen inte laglig.

De rättsliga grunderna för att få behandla personuppgifter är:

- Samtycke
  - Den registrerade har sagt ja till personuppgiftsbehandlingen

  - Generellt sett en olämplig rättslig grund för myndigheter/arbetsgivare (läs mer under rubriken ”samtycke”)
- Avtal med den registrerade
  - Den registrerade har ett avtal eller ska ingå ett avtal med den personuppgiftsansvarige
- Rättslig förpliktelse
  - Det finns lagar och regler som gör att den personuppgiftsansvarige måste behandla vissa personuppgifter.
- Skydda grundläggande intresse
  - Den personuppgiftsansvarige måste behandla personuppgifter för att skydda en registrerad som inte kan lämna samtycke, exempelvis om hen är medvetslös
- Myndighetsutövning och uppgift av allmänt intresse
  - Den personuppgiftsansvarige måste behandla personuppgifter för att utföra sina myndighetsuppgifter eller för att utföra en uppgift av allmänt intresse.
- Intresseavvägning
  - Den personuppgiftsansvarige får behandla personuppgifter om den personuppgiftsansvariges intresse väger tyngre än den registrerades och om behandlingen är nödvändig för det aktuella ändamålet.
  - Kan generellt sett inte användas av myndigheter när myndigheten utför uppgifter som ingår i myndighetens uppdrag.

När VGR behandlar personuppgifter kommer vår rättsliga grund i de flesta fall vara att behandlingen är nödvändig för att:

- fullgöra en rättslig förpliktelse
- fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Vad innebär den rättsliga grunden rättslig förpliktelse?

Rättslig förpliktelse – Behandlingen av personuppgifter har stöd av annan författning. Exempel: Lämna ut uppgifter om anställda till bland annat statliga myndigheter för att redovisa skatter och sociala avgifter beträffande arbetstagarna.

VGR har som offentlig myndighet ett flertal rättsliga förpliktelser som vi måste utföra. Vi har exempelvis en rättslig skyldighet att diarieföra handlingar och registrera vissa personuppgifter i olika ärenden.

Personaladministration innehåller också rättsliga förpliktelser som i sig kräver personuppgiftsbehandling.

Ett annat exempel är att VGR enligt lag har en skyldighet att dokumentera uppgifter som behövs för att tillhandahålla en god och säker vård för patienten, bland annat i våra patientjournaler.

Vad innebär den rättsliga grunden myndighetsutövning och uppgift av allmänt intresse?

Myndighetsutövning och uppgift av allmänt intresse– Gäller när behandlingen av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse. Exempel: Uppgifter som svenska myndigheter måste utföra enligt lag. T.ex. arkivering, forskning och framställning av statistik. Med myndighetsutövning menas ett smalare begrepp än allmänt intresse – närmare bestämt sådana uppgifter som en myndighet enligt lag ska utföra och som har konkreta rättsliga effekter i förhållande till en enskild. Exempel: Ansökan om ekonomiskt bistånd eller bygglov.

För att en arbetsuppgift ska vara av allmänt intresse ska den regleras i svensk lagstiftning eller lagstiftningen inom EU.

VGR:s uppdrag följer av lag, förordningar, föreskrifter och kommunala beslut. Vi har uppdrag inom t.ex. hälso- och sjukvården, kollektivtrafiken, kultur och näringsliv. För att kunna utföra dessa uppgifter av allmänt intresse måste vi i många fall behandla personuppgifter.

Regeringen har varit tydlig med att för att myndigheternas verksamhet ska kunna fungera måste begreppet ”uppgift av allmänt intresse” ges en vid betydelse.

- De obligatoriska uppgifter som åligger kommuner och regioner att utföra är av allmänt intresse.
- Kommuner och regioner har även en långtgående möjlighet att utföra uppgifter på frivillig väg, inom ramen för den kommunala kompetensen. Exempel på sådana uppgifter är att tillhandahålla kulturell verksamhet, konserthus, operahus, fritids- och idrottsanläggningar och åtgärder för att främja det lokala näringslivet. Även sådana uppgifter ingår i allmänintresset.

Exempel på uppgifter av allmänt intresse inom VGR är:

- Hälso- och sjukvården behöver vissa personuppgifter för att kunna erbjuda god och patientsäker vård
- Personuppgifter behöver dokumenteras i patientjournalen
- Bedriva verksamhetsuppföljning och forskning inom vården
- Framställa statistik inom hälso- och sjukvården
- Handlägga ärenden på ett effektivt och rättssäkert sätt
- Ta emot och diarieföra handlingar som skickas in till myndigheten
- Tillgodose allmänhetens rätt att ta del av allmänna handlingar
- Spara allmänna handlingar i myndighetens arkiv
- Sluta avtal med enskilda eller andra organisationer
- Lämna uppgifter till andra myndigheter när detta krävs enligt lag.

Den verksamhet som en region bedriver, inom ramen för sin befogenhet, är av allmänt intresse. En stor del av den behandling av personuppgifter som sker inom VGR följer av lag och bygger alltså på den rättsliga grunden allmänt intresse.

Vad innebär den rättsliga grunden samtycke?

OBS! detta rör samtycke enligt GDPR. Det finns samtycken enligt annan lagstiftning, såsom samtycke till vård eller samtycke till att dela sekretessbelagda uppgifter. Det är inte samma krav för de nämnda olika samtyckena.

Samtycke är generellt en olämplig rättslig grund för myndigheter att stödja sin personuppgiftsbehandling på.

Den registrerade kan när som helst ta tillbaka sitt samtycke. Då måste vi sluta behandla dessa uppgifter. Det blir även ett problem, eftersom vi är en myndighet som inte får radera allmänna handlingar hur som helst.

Ett annat problem med samtycke är administrationen. Det är den personuppgiftsansvarige som ska kunna bevisa att den registrerade har samtyckt. Detta görs lämpligen genom att ha ett skriftligt samtycke som diarieförs. ”Pappers-samtycken” måste förvaras och ordnas så att vi enkelt kan hitta dem om den registrerade återkallar sitt samtycke.

Samtycke kan även vara svårt att använda för offentliga verksamheter eftersom det ofta är ett ojämnt förhållande mellan myndigheten och den registrerade. Detsamma gäller mellan arbetsgivare och arbetstagare.

Om samtycke ändå är lämplig rättslig grund är det viktigt att samtycket följer följande krav:

- Frivilligt – den registrerade måste ha ett reellt och fritt val att lämna eller inte lämna sitt samtycke. Den registrerade ska inte drabbas av några negativa konsekvenser om hen inte lämnar samtycke. Hen får inte heller tvingas till att lämna sitt samtycke – i så fall är det ju inte frivilligt.
- Specifikt – det ska klart och tydligt framgå vad den registrerade samtycker till. Det ska vara precist angivet vad som är syftet med behandlingen. Finns det flera syften ska samtliga syften specificeras så den registrerade har möjlighet att samtycka till alla eller bara några av behandlingarna.
- Informerat – det finns ett minimumkrav på vilken information som den personuppgiftsansvarige, alltså förvaltningen, måste ge den registrerade. För att det ska vara ett giltigt samtycke krävs uppgifter om den personuppgiftsansvariges identitet, syftet med den tänkta behandlingen, vilka uppgifter som behandlas och vilken behandling som är tänkt att äga rum. Den registrerade måste även informeras om att hen har rätt att ta tillbaka sitt samtycke när som helst.
- Otvetydigt – samtycket måste ges aktivt eller genom en förklaring. Det måste vara uppenbart att den registrerade samtyckt till behandlingen i fråga.

Kan VGR använda samtycke för att få hantera personuppgifter i vår verksamhet?

Myndigheter kan i allmänhet inte använda grunden samtycke, utan ska i stället kunna luta sig mot en annan rättslig grund. För VGR är det vanligtvis grunden allmänintresse som gäller.

Enligt GDPR finns inget krav på samtycke om personuppgiftsbehandlingen är ok utifrån annan rättslig grund. I de undantagsfall då vi trots allt bedömer att den rättsliga grunden är samtycke finns regiongemensamma mallar som då ska användas.

Om du tänker behandla personuppgifter med stöd av den rättsliga grunden samtycke, kontakta dataskyddssamordnaren på din förvaltning för rådgivning.

Hur vet jag om en personuppgiftsbehandling är tillåten? ”logisk trappa”

Vilka personuppgifter får man behandla?

En allmän grundregel för att få behandla personuppgifter är att det ska vara nödvändigt. De personuppgifter som samlas in ska vara nödvändiga för ändamålet och därför ska heller inga onödiga personuppgifter samlas in. Nödvändigheten kan härledas från myndighetens grunduppdrag och bör ha stöd i nationella bestämmelser, reglementen eller motsvarande styrdokument.

Ta för vana att fundera över och ifrågasätta vilka personuppgifter som vi verkligen behöver för något som vi ska utföra. Det är sällan ett personnummer behövs på en deltagarlista eller en blankett till exempel. Kanske räcker det med endast namn eller födelseår?

Vad är behandlingsregistret?

Behandlingsregistret är viktigt för att säkerställa att förvaltningen har kontroll över de personuppgifter som behandlas och de behandlingar som dess styrelse/nämnd också är ansvarig för. Behandlingsregistret är en viktig del i att uppfylla GDPR:s krav på transparens och ansvarsskyldighet.

VGR har på central nivå tagit fram ett register över personuppgiftsbehandlingar (även vanligen kallat ”behandlingsregister” eller ”registerförteckning”). Det är Avdelning Säkerhet och Beredskap som ansvarar för den mall som ska användas inom VGR. Det är dock respektive förvaltning som är ansvarig för att hålla den egna förvaltningens behandlingsregister uppdaterat.

Mer information om VGR:s behandlingsregister finns här.

Vilka roller finns det inom dataskydd?

Vem är personuppgiftsansvarig (PUA)?

Den som bestämmer ändamålen för behandlingen av personuppgifterna (varför behandlingen sker) och medlen för behandlingen av personuppgifter (hur behandlingen sker) är personuppgiftsansvarig. Den

personuppgiftsansvarige kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

Inom VGR är varje nämnd och styrelse (enligt nämndens/styrelsens reglemente), personuppgiftsansvarig för de personuppgiftsbehandlingar som sker inom respektive verksamhet. Personuppgiftsansvaret kan inte delegeras till en enskild person. Det är alltså inte en enskild anställd/chef som är ansvarig.

Vad är ett dataskyddsombud och hur kommer jag i kontakt med dataskyddsombudet?

Inom VGR (med undantag för VGR:s bolag) är DSO-teamet utsett dataskyddsombud. DSO-teamet är en central funktion för dataskyddsombud på avdelning juridik, koncernkontoret. Varje förvaltning har en kontaktperson i DSO-teamet.

Ett dataskyddsombud ska till exempel:

- Övervaka personuppgiftsansvarigs efterlevnad av:
  - GDPR
  - annan relevant lagstiftning
  - organisationens dataskyddsstrategi och andra interna styrdokument.
- Informera och ge råd till personuppgiftsansvarig, både de förtroendevalda och anställda som hanterar personuppgifter.
- Ge råd och om möjligt delta vid konsekvensbedömningar.
- Samverka med andra organisationers dataskyddsombud vid behov.
- Ta emot och besvara frågor från registrerade om deras rättigheter och hur dessa kan tillämpas.
- Vara personuppgiftsansvarigs kontaktperson för Integrationsskyddsmyndigheten (IMY).
- Delta vid förhandssamråd med Integrationsskyddsmyndigheten.

Du kan kontakta DSO-teamet på dso@vgregion.se

Dataskyddssamordnare (DSS)

VGR har antagit ett ledningssystem för informationssäkerhet och dataskydd (LISD). Det framgår där att alla förvaltningar ska utse en dataskyddssamordnare (DSS) som bland annat ska vara ett stöd till förvaltningen i dess dataskyddsarbete och verka för en regiongemensam tillämpning av interna styrdokument och regelverk i den egna verksamheten.

Dataskyddskontakt (DSK)

Vissa förvaltningar har förutom dataskyddssamordnare även utsett dataskyddskontakter (DSK). De finns verksamhetsnära och arbetar administrativt med dataskyddsarbetet. Deras arbete samordnas av dataskyddssamordnaren.

Integritetsskyddsmyndigheten (IMY)

Integritetsskyddsmyndigheten är nationell tillsynsmyndighet för efterlevnad av GDPR och annan dataskyddslagstiftning.

I IMYs uppdrag ingår bland annat att granska och kontrollera, ge tillstånd för kreditupplysningsverksamhet, EU-samverkan för en enhetlig tillämpning av GDPR och ge vägledning och sprida kunskap inom dataskyddsområdet.

Läs mer på www.imy.se

Vem riktar IMY en tillsyn mot och vem kan få en sanktionsavgift?

Integritetsskyddsmyndighetens tillsynsärenden riktas mot den personuppgiftsansvarige och inte mot enskilda individer/medarbetare.

IMY kan fatta beslut om olika åtgärder på grund av brister i den personuppgiftsansvariges dataskyddsarbete, exempelvis förelägganden eller sanktionsavgifter.

En myndighet kan få en sanktionsavgift på högst 5 000 000 kronor för mindre allvarliga överträdelser av dataskyddslagstiftningen och högst 10 000 000 kronor för allvarliga överträdelser. Sanktionsavgifter riktas mot den personuppgiftsansvarige, alltså mot styrelsen eller nämnden.

Personuppgiftsbiträde (PUB)

Den personuppgiftsansvarige kan utse ett personuppgiftsbiträde för att utföra vissa personuppgiftsbehandlingar för dess räkning, dvs på uppdrag. Sådana uppdrag kan tex vara utlagda på leverantörer av IT-tjänster. Om man anlitar ett PUB ska alltid ett så kallat PUB-avtal ingås där det finns instruktioner för hur personuppgifterna får behandlas.

Personuppgiftsincidenter

Vad är en personuppgiftsincident?

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Incidenten kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter som överförts, lagrats eller på annat sätt behandlats. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt, det är i båda fall personuppgiftsincidenter.

Vad ska man göra då man upptäcker en misstänkt personuppgiftsincident?

Om du upptäcker en personuppgiftsincident eller misstänker att en personuppgiftsincident inträffat ska du genast rapportera den i MedControl PRO. Om du tror att incidenten är allvarlig ska du kontakta din chef/orsaksutredare och informera dem. Du kan även kontakta dataskyddssamordnaren eller dataskyddsombudet.

Det är viktigt att du rapporterar potentiella personuppgiftsincidenter. Det är ett sätt för förvaltningen att identifiera och åtgärda säkerhetsluckor eller förbättra arbetssätt för att undvika att incidenten händer igen.

Incidenten bedöms och utreds sedan av dataskyddssamordnaren eller liknande funktioner. Du kan komma att kontaktas om fler uppgifter krävs för bedömning och utredning.

Läs mer i VGRs rutin för personuppgiftsincidenter som du hittar här: Rutin - rapportering vid personuppgiftsincidenter

När ska man anmäla en personuppgiftsincident till Integritetskyddmyndigheten? Och informera den registrerade?

Enligt GDPR finns en skyldighet att rapportera personuppgiftsincidenter till Integritetsskyddsmyndigheten (IMY) i vissa fall.

Utgångspunkter vid bedömning om anmälan ska ske till IMY och om information till registrerade

- Risken för registrerade är **osannolik** → Dokumentera internt

- Risken för registrerades rättigheter är **inte osannolik** → Dokumentera internt och rapportera till IMY
- Risken för registrerades rättigheter **är sannolik** → Dokumentera internt och rapportera till IMY samt informera registrerade

Det är den personuppgiftsansvarige, det vill säga den myndighet som bestämmer ändamålen för behandlingen (varför behandlingen sker) av personuppgifterna och medlen för behandlingen (hur behandlingen sker) som gör anmälan till Integritetsskyddsmyndigheten.

Den personuppgiftsansvarige ska utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till Integritetsskyddsmyndigheten.

I begreppet att ha fått vetskap ligger att behörig person/funktion hos personuppgiftsansvarige har fått kännedom om att en incident har inträffat.

Anmälan sker via en E-tjänst på Integritetsskyddsmyndigheten hemsida

Integritetsskyddsmyndigheten skickar efter det en bekräftelse på anmälan.

Anmälda personuppgiftsincidenter kan ligga till grund för en tillsyn från Integritetsskyddsmyndigheten eller till mer allmän information, skriftliga vägledningar mm.

Enligt GDPR måste den personuppgiftsansvarige även informera de registrerade utan onödigt dröjsmål om den personuppgiftsansvarige bedömer att personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

Syftet med att informera de registrerade är att ge dem möjlighet att vidta egna åtgärder för att skydda sig mot negativa konsekvenser eller skador av en personuppgiftsincident.

De registrerade ska informeras efter en bedömning av hur allvarlig konsekvensen är, samt hur sannolikt det är att enskilda personer drabbats av personuppgiftsincidenten.

Observera att man inte alltid måste informera, utan detta får bedömas från fall till fall.

Hur kan vi minimera risken för personuppgiftsincidenter?

Följande åtgärder är exempel på vad som kan göras för att minimera personuppgiftsincidenter.

- Systematiskt säkerhetsarbete
- Vidta organisatoriska och tekniska åtgärder
- Säkerhetsnivån ska sättas i relation till riskerna
- Aktiv behörighetsstyrning

Konsekvensbedömning och förhandssamråd

Vad är en är en konsekvensbedömning?

En konsekvensbedömning är en analys inom dataskydd som genomförs i syfte att ta reda på vilka risker det finns med att behandla personuppgifter vid ett givet ändamål och sammanhang där personuppgifter behandlas. En konsekvensbedömning ska enligt GDPR genomföras om en personuppgiftsbehandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

Läs mer i VGRs rutin här: Konsekvensbedömning avseende dataskydd - Regional rutin 2024-2028.pdf och på IMYs hemsida här: Konsekvensbedömning enligt GDPR | IMY

Vad är ett förhandssamrådråd och när ska vi begära ett sådant?

Om en organisation efter att ha genomfört analyser inom informationssäkerhet och dataskydd, däribland konsekvensbedömning, fortfarande anser att integritetsriskerna efter införda kompenserade åtgärder är alltför höga och den tänkta behandlingen är avgörande för organisationen att implementera ska organisationen innan de påbörjar de tänkta behandlingarna av personuppgifter begära förhandssamrådråd hos Integritetskyddsmyndigheten i syfte att få en extern parts syn på huruvida den tänkta behandlingen utifrån ett integritetsperspektiv kan genomföras. Här kan du både läsa mer om förhandssamråd och begära ett sådant.

Personuppgiftsbiträdesavtal

Vad är ett personuppgiftsbiträde (PUB)?

En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ utanför den egna organisationen som behandlar personuppgifter (hela

eller delar av personuppgiftsbehandlingen) för någon annans (den personuppgiftsansvariges) räkning är personuppgiftsbiträde.

Vad är ett personuppgiftsbiträdesavtal (PUB-avtal)?

Den personuppgiftsansvarige måste teckna ett skriftligt avtal med personuppgiftsbiträdet. Det skriftliga avtalet ska innehålla tydliga instruktioner för behandlingen från den personuppgiftsansvariga till personuppgiftsbiträdet som personuppgiftsbiträdet måste följa.

När ska PUB-avtal tecknas?

Ett personuppgiftsbiträdesavtal (PUB-avtal) ska tecknas när ett personuppgiftsbiträde behandlar personuppgifter för en personuppgiftsansvarigs räkning. Det kan vara att någon part behandlar personuppgifter för VGR:s räkning men också att VGR behandlar personuppgifter för en annan parts räkning.

Ett PUB-avtal tillhör alltid ett huvudavtal. Ett rent inköp av en vara innebär sällan eller aldrig att ett PUB-avtal behöver tecknas, utan som huvudregel är behandling av någon annan parts personuppgifter kopplade till ett inköp av en tjänst.

Innan PUB-avtal tecknas behöver det vara klarlagt att det förhållande som ska regleras verkligen innebär att någon part behandlar personuppgifter och också gör för den andra partens räkning. Något PUB-avtal ska inte tecknas om en behandling inte sker för annan parts räkning, utan sker behandlingen inte för någon annan part är den som utför behandlingen själv personuppgiftsansvarig för dessa behandlingar.

Vem är ansvarig för att PUB-avtal finns

Enligt GDPR är det den personuppgiftsansvarige som har ansvaret för att teckna ett personuppgiftsbiträdesavtal (PUB-avtal) när man anlitar ett personuppgiftsbiträde för att behandla personuppgifter å dennes vägnar.

Det är den personuppgiftsansvarige som bestämmer ändamålen och medlen för behandlingen av personuppgifterna (varför och hur behandlingen ska ske) och alltså också måste säkerställa att behandlingen sker i enlighet med GDPR.

Enligt VGR:s reglemente är respektive styrelse/nämnd personuppgiftsansvarig för styrelsens/nämndens personuppgifter.

Även om det är den personuppgiftsansvarige (i VGR en nämnd/styrelse) som är personuppgiftsansvarig ligger det som utgångspunkt på förvaltningsnivå att

se till att PUB-avtal finns på plats om detta behövs innan en personuppgiftsbehandling påbörjas.

Sker ett inköp genom VGR:s inköpsavdelning ansvarar som huvudregel inköp för att ett PUB-avtal tecknas.

Vem ska teckna PUB-avtal för VGR eller nämnder/förvaltningar i VGR?

Utgångspunkten är att det är den personuppgiftsansvarige som bestämmer ändamålen med behandlingen och medlen för behandlingen (hur behandlingen sker) som är ansvarig för att ett PUB-avtal ingås när förutsättningarna för detta föreligger.

I vissa fall anses regionstyrelsen vara den som är tecknar PUB-avtal för samtliga VGR:s personuppgiftsansvariga styrelser/nämnder. Detta gäller i första hand vid inköp av tjänster som nyttjas av flera av regionens förvaltningar och omfattar behandlingar av regionsöverskridande karaktär.

Utgångspunkten är att det är behörig tjänsteperson hos den personuppgiftsansvarige som har rätt att teckna personuppgiftsbiträdesavtal (PUB-avtal).

Det är inte alltid helt enkelt att avgöra vem som ska skriva på ett PUB-avtal. Vem som är behörig följer av delegationsordningen för respektive förvaltning i VGR. I vissa situationer finns dock tydliga direktiv för att avgöra av vem som har rätt att skriva under ett PUB-avtal.

Vanligtvis uppkommer frågan om PUB-avtal i samband med att en tjänst köps in. Vid upphandling (vilket även omfattar direktupphandling) gäller att den som har behörighet enligt delegationsordningen att teckna huvudavtalet även har behörighet att skriva under tillhörande PUB-avtal. För inköp som går genom Koncerninköp hanteras detta då inom ramen för inköpsprocessen.

Internt inom VGR tecknas inte några PUB-avtal trots att en personuppgiftsansvarig styrelse/nämnd utför behandlingar åt en annan personuppgiftsansvarig styrelse/nämnd. Detta på grund av att VGR är en och samma juridiska person. I stället för PUB-avtal hanteras detta internt. I dagsläget är förfarandet inte exakt dokumenterat (vid frågor om hanteringen av ”PUB-liknande” situationer inom VGR är det Avdelning Säkerhet och Beredskap vid Koncernkontoret som ska kontaktas, detta görs enklast via deras funktionsbrevlåda).

Specifika frågor vid personuppgiftsbehandling

Får vi publicera uppgifter om politiker och fackligt förtroendevalda?

Vi får publicera uppgifter om våra förtroendevalda politiker och fackliga ombud. Det är tillåtet att publicera namn och partitillhörighet på VGR:s förtroendevalda politiker. Det är också tillåtet att publicera namn, facklig tillhörighet och arbetsrelaterade kontaktuppgifter till fackligt förtroendevalda vid exempelvis publicering av en jobbannons.

Bilder, film och ljudinspelning

Hur ska vi tänka kring publicering av bilder, filmer eller ljudinspelningar?

Västra Götalandsregionen har möjlighet att publicera bilder på personer men vi måste följa bestämmelserna i GDPR.

Se GDPR och bilder, filmer och ljudinspelning

En patient/anhörig spelade in vårt samtal, är det ok?

I Sverige är det tillåtet att spela in ett samtal som man själv deltar i och man behöver inte informera de övriga deltagarna om att man spelar in. Om man spelar in samtal som man inte deltar i kan man dock göra sig skyldig till olovlig avlyssning.

Justitieombudsmannen (JO) har i några fall bedömt frågor som rör inspelning mellan patienter och hälso- och sjukvårdspersonal vid vårdtillfällen. JO anser att det ofta finns godtagbara skäl för patienter att spela in ett möte med vårdpersonal, exempelvis för att i efterhand gå igenom läkarens råd eller låta en anhörig ta del av samtalet. JO menar därför att utgångspunkten bör vara att det ska vara tillåtet att göra ljudinspelningar av samtal som patienten själv deltar i.

Läs mer: Fotografering, film- och ljudinspelning vid vårdbesök

En patient/anhörig fotograferar/filmar mig, är det ok?

Ett sjukhus är inte en allmän plats och förvaltningen har rätt att ställa upp regler för dem som visats där. Inom VGR råder det ett generellt fotograferings- och filmningsförbud.

Observera att det kan finnas lokala ordningsregler kring fotografering, filmning och ljudupptagning på de olika förvaltningarna.

Personer som fotograferar eller filmar i hälso- och sjukvårdens verksamheter utan tillstånd ska upplysas om fotoförbudet och uppmanas att avsluta sin aktivitet samt radera bilderna eller filmen. Följer personen inte uppmaningen, ska personen upplysas om att hen kan avvisas från verksamheten såvida vårdbehovet inte föranleder annat. Avvisningen kan ske med bistånd av väktare, ordningsvakt eller polis.

Läs mer: Fotografering, film- och ljudinspelning vid vårdbesök

E-post

Får jag skicka personuppgifter i e-post?

Det som är speciellt med inkommen e-post till skillnad från annan uppgiftshantering är att vi inte kan styra innehållet i den e-post som kommer in. Det är inte ovanligt att personer skriver mail till myndigheten som innehåller mycket personuppgifter, även känsliga sådana om till exempel hälsa.

Om någon skickar känsliga personuppgifter eller sekretessuppgifter innebär det inte att personen har gett sitt samtycke till att hantera personuppgifterna per e-post. Undvik därför att svara genom att skicka med det innehåll som innehåller de känsliga uppgifterna utan ta bort dem i ditt svarsmail.

Tänk på att inte skicka eller spara känsliga personuppgifter i icke krypterad e-post! Hit hör till exempel uppgifter om någons hälsa, religiösa åskådning eller politiska åsikter.

Undvik även att skicka andra integritetskänsliga och extra skyddsvärda uppgifter som exempelvis lönebesked, värderingar av en person såsom social förmåga eller provresultat via e-post.

Om du behöver skicka känsliga personuppgifter

Om du behöver skicka e-post som innehåller känsliga personuppgifter eller sekretessbelagd information krävs att särskilda säkerhetsåtgärder vidtas. Med säkerhetsåtgärder avses i praktiken krypteringsskydd på ett sådant sätt att endast den avsedda mottagaren kan ta del av informationen.

Som huvudregel är det inte tillåtet att skicka känsliga personuppgifter, sekretessmaterial och personnummer.

Det är möjligt att skicka känsliga personuppgifter, sekretessmaterial och personnummer internt inom VGR om vi krypterar e-posten. Läs mer om hur vi krypterar e-post här: Användning av kryptering - Regional rutin 2025 - 2029.pdf och här finner du organisationens generella e-postrutin.

Finns det en säker lösning för meddelanden jag kan använda om jag vill skicka e-post utanför VGR?
Vid Västra Götalandsregionen finns det en tjänst för säker digital kommunikation (SDK) som kan användas Besök gärna länken för mer information om SDK

Kom ihåg, om den information du avser behandla i e-post eller annan digital lösning omfattas av säkerhetsskyddslagen, alltså information som rör riket säkerhet, då ska du **alltid** kontakta Avdelningen för Säkerhet och Beredskap för rådgivning eftersom särskild reglering gäller för den typen av information. Bland annat är det brukligt att utrusning som Försvarsmakten tillhandahåller ska användas, vilket kräver både utbildning och spetskompetens för att få använda.

Du når ASB via: sakerhet-beredskap@vgregion.se

Frågor kopplat till journalen

När får man använda SIEview och NPÖ?

SIEview är en webbapplikation som presenterar journalinformation från Melior i en gemensam läsvy från Meliordatabaser i VGR. Sekretessområdet är den inre sekretessen, inom VGR. Genom SIEview kan man få information från olika söknivåer som ingår inom den egna domänen (motsvarar sjukhus), samtliga anslutna Meliordatabaser i VGR samt även Meliordatabaser som inte längre är i aktivt bruk (arkivdatabaser). Det krävs en vårdrelation med en viss patient och ett syfte att vårda patienten ifråga för att få använda SIEview.

I Nationell Patientöversikt (NPÖ) finns stora mängder journalinformation tillgänglig som delvis kommer utifrån, dvs från vårdgivare som ligger utanför VGRs sekretessområde. Hälso- och sjukvårdspersonal får enligt Socialstyrelsens föreskrift endast ta del av patientuppgifter om de deltar i vården av patienten (eller av något annat ändamål som anges i 2 kap 4 och 5 §§ Patientdatalagen) och behöver uppgifterna för sitt arbete inom hälso- och sjukvården.

För sammanhållen journalföring med exempelvis andra regioner gäller dessutom att uppgifterna rör en patient som det finns en aktuell patientrelation med och att uppgifterna kan antas ha betydelse för att förebygga, utreda eller behandla sjukdomar och skador inom hälso- och sjukvården. För att få åtkomst till sammanhållen journal krävs även att samtycke inhämtas från patienten, eller att det är fråga om nödåtkomst.

Får jag använda uppgifter om patienters hälsa inom forskning?

Det är vanligt att personuppgifter som behandlas för forskningsändamål, såsom uppgifter om hälsa, ursprungligen har samlats in för ett annat ändamål än forskning. Huvudregeln är att personuppgifter ska samlas in för särskilda, uttryckliga angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för bland annat vetenskapliga forskningsändamål ska dock inte anses vara oförenlig med de ursprungliga ändamålen förutsatt att lämpliga skyddsåtgärder används, bl.a. vad gäller uppgiftsminimering, om möjligt pseudonymisering eller anonymisering. För behandling av känsliga personuppgifter i forskningssyfte krävs alltid ett godkännande av etikprövningsmyndigheten alternativt ett beslut av läkemedelsverket ifråga om kliniska prövningar eller medicintekniska produkter.

Kvalitetsregister

Vem ska göra registeranmälan för kvalitetsregister?

Alla personuppgiftsansvariga behöver inte göra registeranmälan för kvalitetsregister. Det är enbart den myndighet som är centralt personuppgiftsansvarig (CPUA) för registerhållningen som ska hantera registerfrågorna. I VGR är det regionstyrelsen som är centralt personuppgiftsansvarig för de flesta registren. Sahlgrenska Universitetssjukhuset är personuppgiftsansvarig för något enstaka register.

Juridiska vägledningar kvalitetsregister | Kunskapsstyrning vård | SKR

När ska informationen om kvalitetsregister lämnas till patienten?

Innan uppgifter om en patient förs in i ett kvalitetsregister ska vårdgivaren informera patienten om detta. Om det inte är möjligt att lämna informationen innan personuppgiftsbehandlingen påbörjas, ska den lämnas så snart som möjligt därefter. Situationen kan uppstå om patienten vårdas akut och uppgifter från vårdtillfället registreras av vårdgivare i ett kvalitetsregister.

Patienten kan vara medvetslös både vid vårdtillfället och rapporteringstillfället. Ett sätt att hantera sådana situationer är att vårdgivare ger patienten information om behandlingen av personuppgifter i ett kvalitetsregister vid utskrivning, i form av en informationsfolder.